

WHAT IS CLAIMED IS:

1. A reverse proxy network communication scheme comprising:
a proxy agent located inside a protected network addressable by a least one internal network device, the proxy agent establishing outgoing network connections;
a security device through which all traffic between the protected network and external networks must travel, the security device permitting at least outgoing connections via at least one predetermined network protocol;
an external proxy server outside the protected network and reachable by the proxy agent via outgoing network connections through the security device, the external proxy server also being addressable by at least one external network device, thereby allowing communication between the at least one external network device and the at least one internal network device.
2. The scheme of claim 1 wherein the at least one predetermined network protocol is HTTP.
3. The scheme of claim 1 further including an outgoing proxy server in communication with the proxy agent and which the proxy agent uses to establish outgoing connections.
4. The scheme of claim 1 wherein the external proxy server is in communication with at least one other network, receives, and stores data addressed to the at least one internal network device.

5. The scheme of claim 4 wherein the proxy agent polls the external proxy server to check for data addressed to the at least one internal network device.

6. The scheme of claim 5 wherein the proxy agent downloads data addressed to the at least one internal network device from the external proxy server and forwards the data to the at least one internal network device.

7. The scheme of claim 4 wherein the external proxy server ensures proper cookie routing.

8. The scheme of claim 1 wherein the proxy agent forwards outgoing data to the external proxy server, which transmits the data to the at least one external network device.

9. A method of accessing an internal network device on a protected network, the network including a security device, the method comprising:

storing data addressed to the internal network device in an external proxy server;

maintaining a proxy agent on the protected network, the proxy agent executing

the step of:

polling the external proxy server for data addressed to the internal network device;

forwarding to the internal network device any data on the external proxy server and addressed to the internal network device; and

forwarding to the external proxy server any data addressed to an external device in communication with the external proxy server.

10. The method of claim 9 further comprising polling the external proxy server at regular intervals.

11. The method of claim 9 further comprising communicating by the internal network device with the external proxy server using a first network protocol and the external network device communicates with the external proxy server using a second network protocol.

12. The method of claim 11 wherein data addressed to the internal network device using the second network protocol is transmitted to the internal device using the first network protocol so that the second network protocol is carried to the internal network device inside the first network protocol.

13. The method of claim 9 further including multiplexing multiple requests from the proxy agent to the external proxy server through the same connection.

14. The method of claim 9 further including maintaining by the external proxy server of maps between local TCP/IP ports of the external proxy server and private IP addresses on the protected network, the maps being distinguished by an identity of the proxy agent used to access them.

15. The method of claim 14 further including publishing by each proxy agent a list of addresses it can reach to the external proxy server, the external proxy server using this list to create a respective map between local ports and proxy agents.

16. The method of claim 14 further including ensuring cookie delivery.

17. The method of claim 9 wherein polling comprises:
connecting to the external proxy server to check for pending traffic;
returning a slow stream of spurious bytes ignored by the proxy agent if there is
nothing pending;
immediately transmitting data from the external proxy server to the proxy agent
when the external proxy server receives data from a client, thus closing
the connection to flush any buffering performed by intervening
(outgoing) proxy servers.

18. The method of claim 9 wherein communication between the proxy agent
and external proxy server is encrypted.

19. The method of claim 18 wherein the data is encrypted using Secure
Sockets Layer (SSL) for HTTP.

20. The method of claim 19 wherein both the proxy agent and the external
proxy server require X.509 certificates.

21. The method of claim 9 further comprising rewriting cookies with unique
identifiers to prevent inadvertent transmission of private information to an incorrect
recipient on the protected network.

22. The method of claim 9 further comprising providing network
administrators control over the system including granting administrators the ability to
allow and deny entry into the protected network on a per session basis.

23. The method of claim 22 wherein access is conferred by granting a key
with a predetermined life span.